

On Massive MIMO Physical Layer Cryptosystem

Ron Steinfeld and Amin Sakzad

Clayton School of Information Technology

Monash University, Melbourne, Victoria, Australia

Emails: ron.steinfeld and amin.sakzad@monash.edu

Abstract—In this paper, we present a zero-forcing (ZF) attack on the physical layer cryptography scheme based on massive multiple-input multiple-output (MIMO). The scheme uses singular value decomposition (SVD) precoder. We show that the eavesdropper can decrypt/decode the information data under the same condition as the legitimate receiver. We then study the advantage for decoding by the legitimate user over the eavesdropper in a generalized scheme using an arbitrary precoder at the transmitter. On the negative side, we show that if the eavesdropper uses a number of receive antennas much larger than the number of legitimate user antennas, then there is no advantage, independent of the precoding scheme employed at the transmitter. On the positive side, for the case where the adversary is limited to have the same number of antennas as legitimate users, we give an $\mathcal{O}(n^2)$ upper bound on the advantage and show that this bound can be approached using an inverse precoder.

Index Terms—Physical Layer Cryptography, Massive MIMO, Zero-Forcing, Singular Value, Precoding.

I. INTRODUCTION

Recently, an interesting new approach for physical security in massive multiple-input multiple-output (MIMO) communication systems was introduced by Dean and Goldsmith [1] and called “Physical layer cryptography”, or a massive MIMO physical layer cryptosystem (MM – PLC). In this scenario, the channel state information (CSI) is known at the legitimate transmitter as well as all the other adversaries and legitimate receivers. The eavesdropper has also the knowledge of the CSI between legitimate users. The idea is to replace the information-theoretic security guarantees of previous physical layer security methods with the weaker complexity-based security guarantees used in cryptography. More precisely, the idea of [1] is to precode the information data at the transmitter, based on the known CSI between the legitimate users, so that the decoding of the received vector would be computationally easy for the legitimate user but computationally hard for the adversary. The goal of this approach is to trade-off a weaker, but still practical, complexity-based security guarantee in order to avoid the less practical additional assumptions required by existing information-theoretic techniques, such as higher noise level in [6], [7], [8] and/or less antennas for the adversary than for legitimate parties in [4], while still retaining the “no secret key” location-based decryption feature of physical-layer security methods.

In [1], a MM – PLC is presented that is claimed to achieve the above goal of the complexity-based approach, using a singular value decomposition (SVD) precoding technique and m -PAM constellations at the transmitter. Namely, it is claimed that, under a certain condition on the number n_t of legitimate sender’s transmit antennas and the noise level β in the adversary’s channel (which we call the *hardness condition* of [1]),

the message decoding problem for the adversary (eavesdropper), termed the MIMO – Search problem in [1], is as hard to solve on average as it is to solve a standard conjectured hard lattice problem in dimension n_t in the worst-case, in particular, the GapSVP_{poly(n_t)} variant of the approximate shortest vector problem in arbitrary lattices of dimension n_t , with approximation factor polynomial in n_t . For these problems, no polynomial-time algorithm is known, and the best known algorithms run in time exponential in the number of transmit antennas n_t , which is typically infeasible when n_t is in the range of few hundreds (as in the case of massive MIMO). Significantly, this computational hardness of MIMO – Search is claimed to hold even if the adversary is allowed to use a large number of receive antennas $n'_r = \text{poly}(n_t)$ polynomially larger than n_t and n_r used by the legitimate parties, and with the same noise level as the legitimate receiver ($\beta = \alpha$). Consequently, under the widely believed conjecture that no polynomial-time algorithms for GapSVP_{poly(n_t)} in dimension n_t exist and the hardness condition of [1], the authors of [1] conclude that their MM – PLC and the corresponding MIMO – Search problem is secure against adversaries with run-time polynomial in n_t .

Our Contribution. In this contribution, we further analyse the complexity-based MM – PLC initiated in [1], to improve the understanding of its potential and limitations. Our contributions are summarized below:

- We show, using a linear receiver known as zero-forcing (ZF) [5], an algorithm with run-time polynomial in n_t for the MIMO – Search problem faced by an adversary against the MM – PLC in [1]. We analyze the decoding success probability of this algorithm and prove that it is $\geq 1 - o(1)$ even if the *hardness condition* of [1] is satisfied, if the ratio $y' = n'_r/n_t$ exceeds a small factor at most logarithmic in n_t , i.e. $y' = \mathcal{O}(\log n_t)$. This contradicts the hardness of the MIMO – Search problem conjectured in [1] to hold for much larger polynomial ratios $y' = \mathcal{O}(\text{poly}(n_t))$. Moreover, we show that the decoding success probability of an adversary against the MM – PLC of [1] using the ZF decoder is approximately the same (or greater than) as the decoding success probability of the legitimate receiver if n'_r is approximately greater than or equal to n_r , assuming an equal noise level for adversary and legitimate receivers. Our first contribution implies that the SVD precoder-based MM – PLC in [1] still requires for security an undesirable assumption limiting n'_r to be less than that of the legitimate receiver, similar to previous information-theoretic techniques.

- As our second contribution, we investigate the potential of the general approach of [1] assuming ZF decoding by the both adversary and legitimate receiver, by studying the generalized scenario where one allows arbitrary precoding matrices by the legitimate transmitter in place of the SVD precoder of the scheme in [1]. To do so, we define a decoding advantage ratio for the legitimate user over the adversary, which is approximately the ratio of the maximum noise power tolerated by the legitimate user's decoder to the maximum noise power tolerated by the adversary's decoder (for the same "high" success probability). We derive a general upper bound on this advantage ratio, and show that, even in the general scenario, the advantage ratio tends to 1 (implying no advantage), if the ratio $n'_r / \max(n_t, n_r)$ exceeds a small constant factor (≤ 9). Thus a linear limitation (in the number of legitimate user antennas) on the number of adversary antennas seems inherent to the security of this approach. On the positive side, we show that, in the case when legitimate parties and the adversary all have the same number of antennas ($n'_r = n_r = n_t$), the upper bound on the advantage ratio is quadratic in n_t and we give experimental evidence that this upper bound can be approximately achieved using an inverse precoder.

Notation. The notation $a \gg b$ denotes that the real number a is much greater than b . We let $|z|$ denotes the absolute value of z . Vectors will be column-wise and denoted by bold small letters. Let \mathbf{v} be a vector, then its j -th entry is represented by v_j . A $k_1 \times k_2$ matrix $\mathbf{X} = [\mathbf{x}_1, \dots, \mathbf{x}_{k_2}]$ is formed by joining the k_1 -dimensional column vectors $\mathbf{x}_1, \dots, \mathbf{x}_{k_2}$. The superscript t denotes transposition operation. We make use of the standard Landau notations to classify the growth of functions. We say that a function $F(n)$ is $\text{poly}(n)$ if it is bounded by a polynomial in n . The notation $\omega(F(n))$ refers to the set of functions (or an arbitrary function in that set) growing faster than $cF(n)$ for any constant $c > 0$. A function $G(n)$ is said negligible if it is proportional to $n^{-\omega(1)}$. If X is a random variable, $\mathbb{P}[X = x]$ denotes the probability of the event " $X = x$ ". The standard Gaussian distribution on \mathbb{R} with zero mean and variance σ^2 is denoted by \mathcal{N}_{σ^2} . We denote by $w \leftarrow \mathcal{D}$ the assignment to random variable w a sample from the probability distribution \mathcal{D} .

II. SYSTEM MODEL

We first summarize the notion of real lattices and SVD (of a matrix) which are essential for the rest of the paper. A k -dimensional *lattice* Λ with a basis set $\{\ell_1, \dots, \ell_k\} \subseteq \mathbb{R}^d$ is the set of all integer linear combinations of basis vectors. Every matrix $\mathbf{M}_{s \times t}$ admits a singular value decomposition (SVD) $\mathbf{M} = \mathbf{U}\mathbf{\Sigma}\mathbf{V}^t$, where the matrices $\mathbf{U}_{s \times s}$ and $\mathbf{V}_{t \times t}$ are two orthogonal matrices and $\mathbf{\Sigma}_{s \times t}$ is a rectangular diagonal matrix with non-negative diagonal elements $\sigma_1(\mathbf{M}) \geq \dots \geq \sigma_s(\mathbf{M})$. By abusing the notation, we denote the Moore-Penrose pseudo-inverse of \mathbf{M} by \mathbf{M}^{-1} , that is $\mathbf{V}\mathbf{\Sigma}^{-1}\mathbf{U}^t$, where the pseudo-inverse of $\mathbf{\Sigma}$ is denoted by $\mathbf{\Sigma}^{-1}$ and can be obtained by taking the reciprocal of each non-zero entry on the diagonal of $\mathbf{\Sigma}$ and finally transposing the matrix.

A. Dean-Goldsmith Model

We consider a slow-fading MIMO wiretap channel model. The $n_r \times n_t$ real-valued MIMO channel from user A to user B is denoted by \mathbf{H} . We also denote the channel from A to the adversary E by an $n'_r \times n_t$ matrix \mathbf{G} . The entries of \mathbf{H} and \mathbf{G} are identically and independently distributed (i.i.d.) based on a Gaussian distribution \mathcal{N}_1 . These channel matrices are assumed to be constant for long time as we employ precoders at the transmitter. This model can be written as:

$$\begin{cases} \mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{e}, \\ \mathbf{y}' = \mathbf{G}\mathbf{x} + \mathbf{e}'. \end{cases}$$

The entries x_i of $\mathbf{x} \in \mathbb{R}^{n_t}$, for $1 \leq i \leq n_t$, are drawn from a constellation $\mathcal{X} = \{0, 1, \dots, m-1\}$ for an integer m . The components of the noise vectors \mathbf{e} and \mathbf{e}' are i.i.d. based on Gaussian distributions $\mathcal{N}_{m^2\alpha^2}$ and $\mathcal{N}_{m^2\beta^2}$, respectively. We assume $\alpha = \beta$ to evaluate the potential of the Dean-Goldsmith model to provide security based on computational complexity assumptions, without a "degraded noise" assumption on the eavesdropper. In this communication setup, the CSI is available at all the transmitter and receivers. In fact, users A and B know the channel matrix \mathbf{H} (via some channel identification process), while adversary E has the knowledge of both channel matrices \mathbf{G} and \mathbf{H} . The knowledge of \mathbf{H} allows A to perform a linear precoding to the message before transmission. More specifically, in [1], to send a message \mathbf{x} to B, user A performs an SVD precoding as follows. Let SVD of \mathbf{H} be given as $\mathbf{H} = \mathbf{U}\mathbf{\Sigma}\mathbf{V}^t$. The user A transmits $\mathbf{V}\mathbf{x}$ instead of \mathbf{x} and B applies a filter matrix \mathbf{U}^t to the received vector \mathbf{y} . With this, the received vectors at B and E are as follows:

$$\begin{cases} \tilde{\mathbf{y}} = \mathbf{\Sigma}\mathbf{x} + \tilde{\mathbf{e}}, \\ \mathbf{y}' = \mathbf{G}\mathbf{V}\mathbf{x} + \mathbf{e}', \end{cases}$$

where $\tilde{\mathbf{e}} = \mathbf{U}^t\mathbf{e}$. Note that since \mathbf{U}^t and \mathbf{V} are both orthogonal matrices, the vector $\tilde{\mathbf{e}}$ and the matrix $\mathbf{G}_v \triangleq \mathbf{G}\mathbf{V}$ continue to be i.i.d. Gaussian vector and matrix, with components of zero mean and variances $m^2\alpha^2$ and 1, respectively.

B. Correctness Condition

Although Dean-Goldsmith do not provide a correctness analysis, we provide one here for completeness. Since $\mathbf{\Sigma} = \text{diag}(\sigma_1(\mathbf{H}), \dots, \sigma_{n_t}(\mathbf{H}))$ is diagonal, user B recovers an estimate \tilde{x}_i of the i -th coordinate/layer x_i of \mathbf{x} , by performing two operations dividing and rounding as follows: $\tilde{x}_i = \lceil \tilde{y}_i / \sigma_i(\mathbf{H}) \rceil = x_i + \lceil \tilde{e}_i / \sigma_i(\mathbf{H}) \rceil$. It is now easy to see that the decoding process succeeds if $|\tilde{e}_i| < |\sigma_i(\mathbf{H})|/2$ for all $1 \leq i \leq n_t$. Since each \tilde{e}_i is distributed as $\mathcal{N}_{m^2\alpha^2}$, the decoding error probability, $\mathbb{P}(\mathbf{B}|\mathbf{H})$ that B incorrectly decodes \mathbf{x} , is, by a union bound, upper bounded by n_t times the probability of decoding error at the worst layer:

$$\begin{aligned} \mathbb{P}(\mathbf{B}|\mathbf{H}) &\leq n_t \mathbb{P}_{w \leftarrow \mathcal{N}_{m^2\alpha^2}}(|w| < |\sigma_{n_t}(\mathbf{H})|/2) \\ &= n_t \mathbb{P}_{w \leftarrow \mathcal{N}_1}(|w| < |\sigma_{n_t}(\mathbf{H})|/(2m\alpha)) \\ &\leq n_t \exp(-|\sigma_{n_t}(\mathbf{H})|^2/(8m^2\alpha^2)), \end{aligned} \quad (1)$$

where we have used the bound $\exp(-x^2/2)$ on the tail of the standard Gaussian distribution. By choosing parameters such that $m^2\alpha^2 \leq |\sigma_{n_t}(\mathbf{H})|^2/(8\log(n_t/\varepsilon))$, one can ensure that B's error probability $\mathbb{P}(\mathbf{B}|\mathbf{H})$ is less than any $\varepsilon > 0$.

C. Security Condition

Unlike decoding by user B, for decoding by the adversary E, the authors of [1] claimed that the complexity of a problem called in [1] the “Search” variant of the “MIMO decoding problem” (to be called MIMO – Search from here on), namely recovering \mathbf{x} from $\mathbf{y}' = \mathbf{G}_v \mathbf{x} + \mathbf{e}'$ and \mathbf{G}_v , with non-negligible probability, under certain parameter settings, upon using massive MIMO systems with large number of transmit antennas n_t , is as hard as solving standard lattice problems in the worst-case. More precisely, it was claimed in [1] that, upon considering above conditions, user E will face an exponential complexity in decoding the message \mathbf{x} . The above cryptosystem is called the *Massive MIMO Physical Layer Cryptosystem* (MM – PLC), and the above problem of recovering \mathbf{x} from \mathbf{y}' is called in [1] the “Search” variant of the “MIMO decoding problem”. For our security analysis, we focus here for simplicity on this MIMO – Search variant. We say that the MIMO – Search problem is *hard* (and the MM – PLC is *secure* in the sense of “one-wayness”) if any attack algorithm against MIMO – Search with run-time $\text{poly}(n_t)$ has negligible success probability $n_t^{-\omega(1)}$. More precisely, in Theorem 1 of [1], a polynomial-time complexity reduction is claimed from worst-case instances of the GapSVP $_{n_t/\alpha}$ problem in arbitrary lattices of dimension n_t , to the MIMO – Search problem with n_t transmit antennas, noise parameter α and constellation size m , assuming the following minimum noise level for the equivalent channel in between A and E holds:

$$m\alpha > \sqrt{n_t}. \quad (2)$$

The reduction is quantum when $m = \text{poly}(n_t)$ and classical when $m = \mathcal{O}(2^{n_t})$, and is claimed to hold for *any polynomial number of receive antennas* $n'_r = \text{poly}(n_t)$. We show in the next Section, however, that in fact for $m\alpha < cn'_r/\sqrt{\log n_t}$ for some constant c , there exists an efficient algorithm for MIMO – Search. Since (2) is independent of the number of receive antennas n'_r , the condition (2) turns out to be not sufficient to provide security of the MM – PLC. We will provide our detailed analysis in the next Section.

III. ZERO-FORCING ATTACK

In this section, we introduce a simple and efficient attack based on ZF linear receivers [5]. We first introduce the attack and analyze its components. The eavesdropper E receives $\mathbf{y}' = \mathbf{G}_v \mathbf{x} + \mathbf{e}'$. Let $\mathbf{G}_v = \mathbf{U}' \Sigma' (\mathbf{V}')^t$ be the SVD of the equivalent channel \mathbf{G}_v . Thus, we get $\mathbf{y}' = \mathbf{U}' \Sigma' (\mathbf{V}')^t \mathbf{x} + \mathbf{e}'$, where both \mathbf{U}' and \mathbf{V}' are orthogonal matrices and Σ' equals $\text{diag}(\sigma_1(\mathbf{G}_v), \dots, \sigma_{n_t}(\mathbf{G}_v)) = \text{diag}(\sigma_1(\mathbf{G}), \dots, \sigma_{n_t}(\mathbf{G}))$, where the last equality holds since the singular values of \mathbf{G}_v and \mathbf{G} are the same. Note that E knows \mathbf{G}_v and its SVD from the assumption that (s)he knows the channel between A and B. At this point, user E performs a ZF attack [5]. S(he) computes

$$\tilde{\mathbf{y}}' = (\mathbf{G}_v)^{-1} \mathbf{y}' = \mathbf{x} + \tilde{\mathbf{e}}', \quad (3)$$

where $\tilde{\mathbf{e}}' = (\mathbf{G}_v)^{-1} \mathbf{e}' = \mathbf{V}' (\Sigma')^{-1} (\mathbf{U}')^t \mathbf{e}'$. User E is now able to recover an estimate \tilde{x}'_i of the i -th coordinate x_i of \mathbf{x} , by rounding: $\tilde{x}'_i = \lceil \tilde{y}'_i \rceil = \lceil x_i + \tilde{e}'_i \rceil = x_i + \lceil \tilde{e}'_i \rceil$.

A. Analysis of ZF Attack

We now investigate the distribution of $\tilde{\mathbf{e}}'$ in (3).

Lemma 1: The components of $\tilde{\mathbf{e}}'$ in (3) are distributed as $\mathcal{N}_{\sigma_E^2}$ with $\sigma_E^2 \leq (m^2 \alpha^2) / \sigma_{n_t}^2(\mathbf{G})$.

Proof: Note that $(\mathbf{U}')^t \mathbf{e}'$ has the same distribution as \mathbf{e}' since $(\mathbf{U}')^t$ is orthogonal. Hence, z_j , the j -th coordinate of the vector $\mathbf{z} = (\Sigma')^{-1} (\mathbf{U}')^t \mathbf{e}'$ is distributed as $\mathcal{N}_{m^2 \alpha^2 / \sigma_j^2(\mathbf{G})}$, for all $1 \leq j \leq n_t$. We also note that z_j 's are independent with different variances. Now let \mathbf{v}'_i denotes the i -th row of \mathbf{V}' . We find the distribution of

$$t_i = \langle \mathbf{v}'_i, \mathbf{z} \rangle = \sum_{j=1}^{n_t} v'_{i,j} z_j. \quad (4)$$

Since the linear combination at (4) is distributed as a linear combination of independent Gaussian distributions, t_i is distributed as

$$\sum_{j=1}^{n_t} v'_{i,j} \mathcal{N}_{m^2 \alpha^2 / \sigma_j^2(\mathbf{G})} = \mathcal{N}_{\sum_{j=1}^{n_t} |v'_{i,j}|^2 m^2 \alpha^2 / \sigma_j^2(\mathbf{G})} \quad (5)$$

$$= \mathcal{N}_{m^2 \alpha^2 \sum_{j=1}^{n_t} |v'_{i,j}|^2 / \sigma_j^2(\mathbf{G})}. \quad (6)$$

Since $\sigma_j^2(\mathbf{G}) \geq \sigma_{n_t}^2(\mathbf{G})$, for all $1 \leq j \leq n_t$, the random variable t_i is distributed as $\mathcal{N}_{\sigma_{t_i}^2}$ with

$$\sigma_{t_i}^2 = m^2 \alpha^2 \sum_{j=1}^{n_t} \frac{|v'_{i,j}|^2}{\sigma_j^2(\mathbf{G})} \leq \frac{m^2 \alpha^2}{\sigma_{n_t}^2(\mathbf{G})} \sum_{j=1}^{n_t} |v'_{i,j}|^2 = \frac{m^2 \alpha^2}{\sigma_{n_t}^2(\mathbf{G})}, \quad (7)$$

where the last equality holds because \mathbf{V}' is orthogonal. ■ The above explained ZF attack succeeds if $|\tilde{e}'_i| < 1/2$ for all $1 \leq i \leq n_t$. Let $\mathbb{P}_{\text{ZF}}(\mathbf{E}|\mathbf{G})$ denotes the decoding error probability that E incorrectly recovers \mathbf{x} using ZF attack. Based on Lemma 1, we have

$$\begin{aligned} \mathbb{P}_{\text{ZF}}(\mathbf{E}|\mathbf{G}) &\leq n_t \mathbb{P}_{w \leftarrow \mathcal{N}_{\sigma_E^2}}(|w| < 1/2) \\ &\leq n_t \mathbb{P}_{w \leftarrow \mathcal{N}_1}(|w| < |\sigma_{n_t}(\mathbf{G})| / (2m\alpha)). \end{aligned} \quad (8)$$

By comparing (1) and (8), we see that the noise conditions for decoding \mathbf{x} by users B and E are the same if both users have the same number of receive antennas $n'_r = n_r$ and the distributions of channels \mathbf{G} and \mathbf{H} are the same. This implies that user E is able to decode under the same constraints/conditions as B. Moreover, if $n'_r > n_r$, then the adversary E is capable of decoding higher noise.

B. Asymptotic Probability of Error for Adversary

Before starting this section, we mention a Theorem from [3] regarding the least/largest singular value of matrix variate Gaussian distribution. This theorem relates the least/largest singular value of a Gaussian matrix to the number of its columns and rows asymptotically.

Theorem 1 ([3]): Let \mathbf{M} be an $s \times t$ matrix with i.i.d. entries distributed as \mathcal{N}_1 . If s and t tend to infinity in such a way that s/t tends to a limit $y \in [1, \infty]$, then

$$\sigma_t^2(\mathbf{M})/s \rightarrow \left(1 - \sqrt{1/y}\right)^2 \quad (9)$$

and

$$\sigma_1^2(\mathbf{M})/s \rightarrow \left(1 + \sqrt{1/y}\right)^2, \quad (10)$$

almost surely.

We now analyze the asymptotic probability of error for eavesdropper using a ZF linear receiver.

Theorem 2: Fix any real $\varepsilon, \varepsilon' > 0$, and $y' \in [1, \infty]$, and suppose that $n'_r/n_t \rightarrow y'$ as $n_t \rightarrow \infty$. Then, for all sufficiently large n_t , the probability $\mathbb{P}_{\text{ZF}}(\text{E})$ that E incorrectly decodes the message \mathbf{x} using a ZF decoder is upper bounded by ε , if

$$m^2 \alpha^2 \leq \frac{n'_r \left((1 - \sqrt{1/y'})^2 - \varepsilon' \right)}{8 \log(2n_t/\varepsilon)}. \quad (11)$$

Proof: Let \mathcal{G} be the set of all channel matrices \mathbf{G} such that $\sigma_{n_t}^2(\mathbf{G}) \geq n'_r \left((1 - \sqrt{1/y'})^2 - \varepsilon' \right)$. Note that $\mathbf{G} \notin \mathcal{G}$ with vanishing probability $o(1)$ as $n_t \rightarrow \infty$, by Theorem 1. We have:

$$\begin{aligned} \mathbb{P}_{\text{ZF}}(\text{E}) &= \mathbb{P}_{\text{ZF}}(\text{E}|\mathbf{G} \in \mathcal{G})\mathbb{P}(\mathbf{G} \in \mathcal{G}) + \mathbb{P}_{\text{ZF}}(\text{E}|\mathbf{G} \notin \mathcal{G})\mathbb{P}(\mathbf{G} \notin \mathcal{G}) \\ &\leq \mathbb{P}_{\text{ZF}}(\text{E}|\mathbf{G} \in \mathcal{G}) + \mathbb{P}(\mathbf{G} \notin \mathcal{G}) \\ &\leq n_t \mathbb{P}_{w \leftarrow \mathcal{N}_1}(|w| < |\sigma_{n_t}(\mathbf{G})|/(2m\alpha)) + o(1) \\ &\leq n_t \exp(-\sigma_{n_t}^2(\mathbf{G})/(8m^2\alpha^2)) + o(1) \\ &\leq n_t \exp\left(\frac{-n'_r((1 - \sqrt{1/y'})^2 - \varepsilon')}{8m^2\alpha^2}\right) + o(1), \end{aligned}$$

where the first inequality is due the facts that $\mathbb{P}(\mathbf{G} \in \mathcal{G}) \leq 1$ and $\mathbb{P}_{\text{ZF}}(\text{E}|\mathbf{G} \notin \mathcal{G})\mathbb{P}(\mathbf{G} \notin \mathcal{G}) \leq \mathbb{P}(\mathbf{G} \notin \mathcal{G})$, the second inequality is true based on (8) and Theorem 1, the third inequality uses the well-known upper bound $\exp(-x^2/2)$ for the tail of a Gaussian distribution and the last inequality follows from the definition of \mathcal{G} . By letting $\mathbb{P}_{\text{ZF}}(\text{E}) \leq \varepsilon$, the sufficient condition (11) can be obtained. ■

Comparing conditions (2) and (11), we conclude that if y' exceeds a small factor at most logarithmic in n_t , i.e. $y' = \mathcal{O}(\log n_t)$ we can have both conditions satisfied and yet Theorem 2 shows that MIMO – Search can be efficiently solved, i.e. this contradicts the hardness of the MIMO – Search problem conjectured in [1] to hold for much larger polynomial ratios $y' = \mathcal{O}(\text{poly}(n_t))$.

To analytically investigate the advantage of decoding at B over E, we define the following advantage ratio.

Definition 1: For fixed channel matrices \mathbf{H} and \mathbf{G} , the ratio

$$\text{adv} \triangleq \sigma_{n_t}^2(\mathbf{H})/\sigma_{n_t}^2(\mathbf{G}), \quad (12)$$

is called the advantage of B over E.

We note from (1) and (8) that adv is the ratio between the maximum noise power tolerated by B's ZF decoder to the maximum noise power tolerated by E's ZF decoder, for the same decoding error probability in both cases. First, we study this advantage ratio asymptotically. We use Theorem 1 to obtain the following result.

Proposition 1: Let $\mathbf{H}_{n_r \times n_t}$ be the channel between A and B and $\mathbf{G}_{n'_r \times n_t}$ be the channel between A and E, both with i.i.d. elements each with distribution \mathcal{N}_1 . Fix real $y, y' \in [1, \infty]$, and suppose that $n_r/n_t \rightarrow y$ and $n'_r/n_t \rightarrow y'$ as $n_t \rightarrow \infty$. Then, using a SVD precoding technique in MM – PLC, we have $\text{adv} \rightarrow (\sqrt{y} - 1)^2 / (\sqrt{y'} - 1)^2$ almost surely as $n_t \rightarrow \infty$.

Proof: Based on Theorem 1 for \mathbf{H} and \mathbf{G} , we have

$$\begin{cases} \sigma_{n_t}^2(\mathbf{H})/n_r \rightarrow (1 - \sqrt{1/y})^2 \\ \sigma_{n_t}^2(\mathbf{G})/n'_r \rightarrow (1 - \sqrt{1/y'})^2. \end{cases}$$

Substituting the above two limits into (12) and using $n_r/n'_r = (n_r/n_t)/(n'_r/n_t) \rightarrow y/y'$, the result follows. ■

Note that $\text{adv} \rightarrow 1$ is obtained in the case that $y = y'$, which is equivalent to $n_r/n'_r \rightarrow 1$. On the other hand $\text{adv} \rightarrow 0$, if $y'/y = \infty$ which is equivalent to $n'_r/n_r \rightarrow \infty$.

C. General Precoding Scheme

One may wonder whether a different precoding method (again, assumed known to E) than used above may provide a better advantage ratio for B over E. Suppose that instead of sending $\tilde{\mathbf{x}} = \mathbf{V}\mathbf{x}$, user A precodes $\tilde{\mathbf{x}} = \mathbf{P}(\mathbf{H})\mathbf{x}$, where $\mathbf{P} = \mathbf{P}(\mathbf{H})$ is some other precoding matrix that depends on the channel matrix \mathbf{H} . Then, given the channel matrices, the analysis given in Section III shows that using ZF decoding, B's decoding error probability will be bounded as $n_t \exp(-\sigma_{n_t}^2(\mathbf{HP})/(8m^2\alpha^2))$, while E's decoding error probability will be bounded as $n_t \exp(-\sigma_{n_t}^2(\mathbf{GP})/(8m^2\alpha^2))$. Therefore, in this general case, the advantage ratio of maximum noise power decodable by B to that decodable by E at a given error probability generalizes from (12) to

$$\text{adv} \triangleq \sigma_{n_t}^2(\mathbf{HP})/\sigma_{n_t}^2(\mathbf{GP}). \quad (13)$$

We now give an upper bound on the advantage ratio (13). Let us first define

$$\text{advup} \triangleq \frac{\sigma_1^2(\mathbf{H})}{\sigma_{n_t}^2(\mathbf{G})}.$$

Proposition 2: Let \mathbf{H} and \mathbf{G} be as in Proposition 1. Then we have $\text{adv} \leq \text{advup}$. Furthermore, fix real $y, y' \in [1, \infty]$, and suppose that $n_r/n_t \rightarrow y$ and $n'_r/n_t \rightarrow y'$ as $n_t \rightarrow \infty$, so that $n'_r/n_r \rightarrow y'/y \triangleq \rho'$. Then, using a general precoding matrix $\mathbf{P}(\mathbf{H})$ in MM – PLC, we have $\text{advup} \rightarrow (\sqrt{y} + 1) / (\sqrt{y'} - 1)^2$ almost surely as $n_t \rightarrow \infty$. Hence, in the case $n'_r = n_r$ and $y' = y \rightarrow \infty$, we have $\text{advup} \rightarrow 1$. Moreover, if $\text{advup} \rightarrow c$ for some $c \geq 1$, then $\min(y', \rho') \leq 9$.

Proof: It is easy to see the two inequalities below hold for every \mathbf{H} , \mathbf{G} , and \mathbf{P} :

$$\begin{cases} \sigma_{n_t}(\mathbf{HP}) \leq \sigma_1(\mathbf{H})\sigma_{n_t}(\mathbf{P}), \\ \sigma_{n_t}(\mathbf{GP}) \geq \sigma_{n_t}(\mathbf{G})\sigma_{n_t}(\mathbf{P}). \end{cases}$$

Hence, the advantage ratio (13) can be upper bounded as

$$\text{adv} \leq \frac{\sigma_1^2(\mathbf{H})\sigma_{n_t}^2(\mathbf{P})}{\sigma_{n_t}^2(\mathbf{G})\sigma_{n_t}^2(\mathbf{P})} = \frac{\sigma_1^2(\mathbf{H})}{\sigma_{n_t}^2(\mathbf{G})} = \text{advup}. \quad (14)$$

Using Theorem 1 for the the numerator and the denominator of the RHS of (14), respectively, and $n_r/n'_r \rightarrow y/y'$, we get

$$\text{advup} \rightarrow \frac{y(1 + \sqrt{1/y})^2}{y'(1 - \sqrt{1/y'})^2} = \left(\frac{\sqrt{y} + 1}{\sqrt{y'} - 1} \right)^2.$$

In the case $n'_r = n_r$ and $y = y' \rightarrow \infty$, the latter inequality gives $\text{advup} \rightarrow 1$. Also, the inequality $(\sqrt{y} + 1) / (\sqrt{y'} - 1)^2 \geq 1$ implies (using $y = y'/\rho'$) that $\rho' \leq 1/(1 - 2/\sqrt{y'})^2$, and the RHS of the latter is ≤ 9 for all $y' \geq 9$, which implies $\min(y', \rho') \leq 9$. ■

IV. ACHIEVABLE UPPER BOUND ON ADVANTAGE RATIO

The above analysis shows that one cannot hope to achieve an advantage ratio greater than 1, if the the adversary uses

a number of antennas significantly larger than used by the legitimate parties (by more than a constant factor). We now explore what advantage ratio can achieve if we add a new constraint to MM – PLC, namely the number of adversary antennas is limited to be the same as the number of legitimate transmit and receive antennas. That is, we study the advantage ratio when the channel matrices \mathbf{H} and \mathbf{G} are square matrices and not rectangular. We show that under this simple constraint $n = n_t = n_r = n'_r$, the advantage ratio is capable of getting larger than 1 and as big as $\mathcal{O}(n^2)$. We employ the following result in our analysis.

Theorem 3 ([3]): Let \mathbf{M} be a $t \times t$ matrix with i.i.d. entries distributed as \mathcal{N}_1 . The least singular value of \mathbf{M} satisfies

$$\lim_{t \rightarrow \infty} \mathbb{P} \left[\sqrt{t} \sigma_t(\mathbf{M}) \geq x \right] = \exp(-x^2/2 - x). \quad (15)$$

We note that for a similar result on the largest singular value for square matrices, Theorem 1 is enough. Using the above Theorem along with Theorem 1, one can further upper bound and estimate the advantage ratio. More precisely, we have

$$\text{adv} \leq \sigma_1^2(\mathbf{H})/\sigma_n^2(\mathbf{G}) \quad (16)$$

$$\rightarrow 4n/\sigma_n^2(\mathbf{G}) = 4n^2/(n\sigma_n^2(\mathbf{G})), \quad (17)$$

where (16) is obtained based on (14). As $n \rightarrow \infty$, based on Theorem 3, the denominator of the RHS of (17) is $\mathcal{O}(1)$ except with probability $\leq \varepsilon$ for any fixed $\varepsilon > 0$, and thus adv is $\mathcal{O}(n^2)$ with the same probability. The following proposition is now outstanding.

Proposition 3: Let $\varepsilon > 0$ be fixed, \mathbf{H} and \mathbf{G} be $n \times n$ matrices as in Proposition 1 with $n = n_t = n_r = n'_r$. Using a general precoder $\mathbf{P}(\mathbf{H})$ to send the plain text \mathbf{x} , the maximum possible adv that B can achieve over E, is of order $\mathcal{O}(n^2)$, except with probability $\leq \varepsilon$.

The above proposition implies that user B *may* be able to decode the message \mathbf{x} , with noise power up to n^2 times greater than E is able to handle. Such an advantage was not available in MM – PLC scheme proposed in [1] due to the lack of constraint on the number of receive antennas for E and the use of SVD precoder. We present below experimental evidence that this upper bound can be approached using an *inverse* precoder $\mathbf{P}(\mathbf{H}) = \mathbf{H}^{-1}$. This inverse precoder may not be power efficient as it may need a lot of power enhancement at A, however it gives us a benchmark on the achievable advantage ratio. In this framework, the equivalent channel between legitimate users is the identity matrix and the channel between users A and E is $\mathbf{G}\mathbf{H}^{-1}$. In Fig. 1, we have shown the value of $\log_{10}(\text{adv})$ for 1000 square channel matrices of size $n = 200$. For reference, we also plot the mean value along with $\log_{10}(200^2)$. Clearly, in most cases the advantage ratio (12) is within a small factor (compared to n^2) of n^2 .

V. SUMMARY AND DIRECTIONS FOR FUTURE WORK

Our results suggest several natural open problems for future work. The implied contradiction between our first contribution and the conjectured hardness of MIMO – Search in [1] for $n'_r/n_t = \mathcal{O}(\text{poly}(n_t))$ implies either a polynomial-time algorithm for worst-case GapSVP_{poly(n_t)} or that the complexity reduction of [1] (Theorem 1 of [1]) between MIMO – Search and GapSVP_{poly(n_t)} does not hold under the

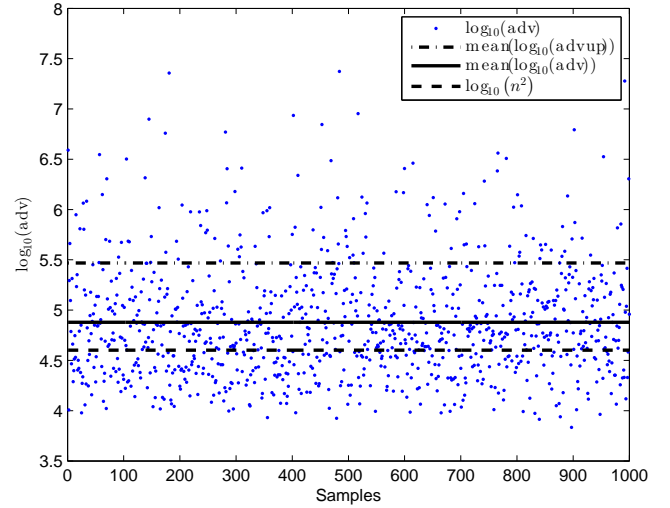


Fig. 1. The advantage ratio (12) for 1000 square channels of size $n = 200$ using inverse precoder.

hardness condition of [1]. We believe the second possibility is the correct one, and that there is a gap in the proof of Theorem 1 of [1]. We do not yet know if the gap can be filled to give a worst-case to average-case reduction under a revised hardness condition. This is left for future work.

Our generalized upper bound on legitimate user to adversary ZF decoding advantage suggests the complexity-based approach does not remove the needed linear limitation on the number of adversary antennas versus the number of legitimate party antennas, that is also suffered by previous information-theoretic methods. Can a more general complexity-based approach to physical-layer security avoid this limitation?

Finally, our positive result for the inverse precoder suggests that if the adversary is limited to have the same number of antennas as the legitimate parties, the complexity-based approach may provide practical security. This suggests the following questions: How secure is this inverse precoding scheme against more general decoding attacks (other than ZF)? Can a security reduction from a worst-case standard lattice problem be given for this case? How does the practicality of the resulting scheme compare to existing physical-layer security schemes based on information-theoretic security arguments? Can the efficiency of those schemes be improved by the complexity-based approach?

REFERENCES

- [1] T. Dean and A. Goldsmith, "Physical-layer cryptography through massive MIMO," *Information Theory Workshop (ITW), 2013 IEEE*, pp. 1–5, 9–13 Sept. 2013. Extended version is also available online at: <http://arxiv.org/abs/1310.1861>.
- [2] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. on Inform. Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976.
- [3] A. Edelman, "Eigenvalues and Condition Numbers of Random Matrices," *M.I.T. Doctoral Dissertation, Mathematics Department*, 1989.
- [4] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. on Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
- [5] K. Kumar, G. Caire, and A. Moustakas, "Asymptotic performance of linear receivers in MIMO fading channels," *IEEE Trans. on Inform. Theory*, vol. 55, no. 10, pp. 4398–4418, Oct. 2009.
- [6] F. Oggier and B. Hassibi, "The Secrecy Capacity of the MIMO Wiretap Channel," *IEEE Trans. on Inform. Theory*, vol. 57, no. 8, pp. 4961–4972, Oct. 2011.
- [7] J. Zhu, R. Schober, and V. Bhargava, "Secure transmission in multicell massive MIMO systems," *Globecom Workshops (GC Wkshps), 2013 IEEE*, pp. 1286–1291, 9–13 Dec. 2013.

- [8] J. Wang, J. Lee, F. Wang, and T. Quek, "Secure communication via jamming in massive MIMO Rician channels," *Globecom Workshops (GC Wkshps)*, 2013 IEEE, pp. 340–345, 8–12 Dec. 2014.
- [9] A.D. Wyner, "The Wire-Tap Channel," *Bell System Technical Journal*, vol. 54, Issue. 8 pp. 1355–1387, Oct. 1975.